WILLKIE FARR & GALLAGHER LLP
BENEDICT Y. HUR (SBN 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN 246943)
sagnolucci@willkie.com
EDUARDO E. SANTACANA (SBN 281668)
esantacana@willkie.com
TIFFANY LIN (SBN 321472)
tlin@willkie.com
YUHAN ALICE CHI (SBN 324072)
ychi@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

JANE DOE, JANE DOE II, JOHN DOE, E.C., JOSE MARQUEZ, and HOLLIS WILSON, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOODRX HOLDINGS, INC., CRITEO CORP., META PLATFORMS, INC., AND GOOGLE LLC,

Defendants.

Case Nos. 3:23-cv-00501-AMO

DEFENDANT GOOGLE, LLC'S STATEMENT OF RECENT DECISION

Consolidated Complaint Filed: May 26, 2023

Date: June 12, 2025
Time: 2:00 PM
Location: Courtroom 10, 19th Floor
Judge: Hon. Araceli Martínez-Olguín

DEFENDANT GOOGLE LLC'S STATEMENT OF RECENT DECISION

Pursuant to Civil Local Rule 7-3(d)(2), Defendant Google LLC ("Google") respectfully submits for the Court's consideration the recent Order Granting Defendant's Motion for Summary Judgment in *Torres v. Prudential Fin., Inc.*, No. 22-CV-07465 (CRB), 2025 WL 1135088 (N.D. Cal. Apr. 17, 2025), a true and correct copy of which is attached hereto as Exhibit A. The decision is relevant to Plaintiffs' claim for violation of the California Invasion of Privacy Act ("CIPA"), California Penal Code § 631, which Google has moved to dismiss (ECF No. 213).

Dated: May 27, 2025

WILLKIE FARR & GALLAGHER LLP

By: */s/ Benedict Y. Hur*
Benedict Y. Hur
Simona A. Agnolucci
Eduardo E. Santacana
Tiffany Lin
Yuhan Alice Chi

Attorneys for Defendant Google LLC

EXHIBIT A

2025 WL 1135088
Only the Westlaw citation is currently available.
United States District Court, N.D. California.

Valerie TORRES and Rhonda Hyman, et al., Plaintiffs,
v.
PRUDENTIAL FINANCIAL, INC., ActiveProspect, Inc., and Assurance IQ, LLC., Defendants.

Case No. 22-cv-07465 (CRB)
|
Signed April 17, 2025

Attorneys and Law Firms

Adam E. Polk, Simon Seiver Grille, Dena C. Sharp, Nina Gliozzo, Girard Sharp LLP, San Francisco, CA, for Plaintiffs Tyrone Hazel, Roxane Evans.

Adam E. Polk, Simon Seiver Grille, Dena C. Sharp, Jordan Nadine Isern, Nina Gliozzo, Girard Sharp LLP, San Francisco, CA, for Plaintiffs Valerie Torres, Rhonda Hyman.

Kelly Max Klaus, Jonathan Hugh Blavin, Virginia Grace Davis, Munger Tolles & Olson LLP, San Francisco, CA, Laura Danielle Smolowe, Akin Gump Strauss Hauer & Feld LLP, Los Angeles, CA, Sidney M. Eisner, Munger, Tolles & Olson LLP, Los Angeles, CA, for Defendant Prudential Financial, Inc.

Kelly Max Klaus, Virginia Grace Davis, Munger Tolles & Olson LLP, San Francisco, CA, Laura Danielle Smolowe, Akin Gump Strauss Hauer & Feld LLP, Los Angeles, CA, Sidney M. Eisner, Munger, Tolles & Olson LLP, Los Angeles, CA, for Defendants ActiveProspect, Inc., Assurance IQ, LLC.

ORDER GRANTING MOTION FOR SUMMARY JUDGMENT

CHARLES R. BREYER, United States District Judge

***1** This action is the latest in a line of cases challenging the use of third-party software to record website visitor activity without their knowledge. Plaintiffs sue Defendants ActiveProspect, Prudential Financial, and Assurance IQ, alleging that ActiveProspect violated the California Invasion of Privacy Act by intercepting, recording, and storing real-time interactions with a webform on Prudential's website without consent. Plaintiffs further allege that Prudential and Assurance violated CIPA by employing ActiveProspect and embedding its software services on the Prudential website without proper disclosure to website users. Defendants move for summary judgment on the basis that there is no genuine dispute of material fact as to whether ActiveProspect read or attempted to read the contents of Plaintiffs' communications while they were in transit, as is required to establish a section 631 CIPA violation. The Court **GRANTS** Defendants' motion.

I. BACKGROUND

A. Factual History

Prudential and its wholly owned subsidiary Assurance designed and operated an online webform for people to fill out in order to obtain a life insurance quote. SAC (dkt. 56) ¶ 1. The webform prompted users to enter information about their demographics, family situation, and medical history. Id. ¶ 45. Prudential and Assurance employed the software vendor ActiveProspect and embedded its software product "TrustedForm" into the source code of the webform. Id. ¶¶ 43, 47; Mot. (dkt. 93) at 2.

The moment a user interacted with the webform, TrustedForm collected user metadata and recorded the interaction using a software tool called "event listeners." Polish Decl. (dkt. 93-30) ¶ 32; Wolfe Decl. (dkt. 93-29) ¶¶ 15, 19. Event listeners detect button clicks, mouse movements, and keyboard inputs. Polish Decl. ¶ 32. TrustedForm then generates a "TrustedForm Certificate" that contains the event data and sends a corresponding "TrustedForm Certificate URL" to the website owner. Wolfe Decl. ¶¶ 9, 13. Each TrustedForm Certificate includes a "session replay," which is a recreation of the events that took place on the webform including, but not limited to, any user-submitted data. Rafferty Dep. (dkt. 105-3) at 26:19–27:22; Wolfe Decl. ¶ 14.

TrustedForm Certificates are encrypted and transmitted to ActiveProspect's servers for storage. Wolfe Decl. ¶ 17. Some values in the webform, like emails, are normalized and hashed prior to transmission to the servers. Williams Dep. (dkt. 105-5) at 174:12–24. To retrieve a TrustedForm Certificate, the website owner must have the associated TrustedForm Certificate URL. Wolfe Decl. ¶ 44–45. So, for example, Prudential and Assurance can claim and retrieve a TrustedForm Certificate through their TrustedForm accounts by clicking the associated TrustedForm Certificate URL that is sent to them when the TrustedForm Certificate is created. Id. ¶ 37.

Select ActiveProspect employees are "superusers" who can access the accounts of accountholders and also view TrustedForm Certificates and session replays. Wolfe Dep. (dkt. 105-8) at 162:14–163:2, 145:15–146:13. As far as the record reveals, these employees access TrustedForm accounts only for troubleshooting purposes. Wolfe Dep. at 162:21–25; Williams Dep. at 123:11–124:10.

***2** Between December 2021 and January 2023, Plaintiffs visited the webform and 2 entered the requested information to obtain a life insurance quote. SAC ¶¶ 67, 71. Prudential did not expressly disclose to Plaintiffs that ActiveProspect was recording their interactions with the form until Plaintiffs had already completed the form and clicked "Get an instant quote." Id. ¶¶ 53, 54, 58. Plaintiffs assert that at the time they filled out the form, they were not aware of and did not consent to ActiveProspect's interception and collection of their information, which of course went beyond the information that they input into the form and included keystrokes, mouse clicks, and data inputs. Id. ¶¶ 70, 74.

B. Procedural History

In November 2022, Plaintiffs filed a class action complaint alleging that Defendants' use of TrustedForm violated section 631 of CIPA, the California Unfair Competition Law, and Article 1 of the California Constitution. Compl. (dkt. 1). Defendants moved to dismiss Plaintiffs' claims. MTD (dkt. 21). The Court dismissed Plaintiffs' UCL claim but held that Plaintiffs had alleged sufficient facts to plausibly state invasion of privacy claims under section 631 and the California Constitution. Order (dkt. 29) at 11. Plaintiffs filed their Second Amended Complaint (SAC) on June 6, 2024.

On June 28, 2024, Plaintiffs sought class certification solely for their section 631 claim. Mot. for Class Cert. (dkt. 66). The Court granted Plaintiffs' motion. Order Granting Class Cert. (dkt. 97). In October 2024, the parties agreed to allow Defendants to file the instant early summary judgment motion specifically as to legal issues that would not require additional factual development. Joint Stip. (dkt. 86).

II. LEGAL STANDARD

Summary judgment is proper when there is "no genuine dispute as to any material fact and the [moving party] is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). Material facts are those that may affect the outcome of the case. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986). A dispute is genuine if "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." Id.

The moving party bears the initial burden of identifying those portions of the pleadings, discovery, and affidavits that demonstrate the absence of a genuine issue of material fact. Celotex Corp. v. Cattrett, 477 U.S. 317, 323 (1986). Once the moving party meets its initial burden, the nonmoving party must go beyond the pleadings to demonstrate the existence of a genuine dispute of material fact by "citing to particular parts of materials in the record" or "showing that the materials cited do not establish the absence or presence of a genuine dispute." Fed. R. Civ. P. 56(c). If the nonmoving party fails to do so, "the moving party is entitled to a judgment as a matter of law." Celotex, 477 U.S. at 323.

III. DISCUSSION

The second prong of section 631 imposes liability where a person, "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit." Cal. Penal Code § 631. Defendants make two arguments as to why they cannot be liable under section 631. First, Defendants argue that ActiveProspect does not constitute a third-party eavesdropper. Mot. at 12–20. Second, Defendants argue that ActiveProspect did not read or attempt to read Plaintiffs' communications while the communications were in transit. Id. at 21–24.

A. Third-Party Eavesdropper

Liability under the second prong of section 631 attaches "only to eavesdropping by a third party and not to recording by a participant to a conversation." Warden v. Kahn, 99 Cal. App. 3d 805, 811 (1979); In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 607 (9th Cir. 2020). A third-party eavesdropper under section 631 is one who secretly listens to conversations between two other parties or who receives "simultaneous dissemination" of the "contents of a conversation." Ribas v. Clark, 38 Cal. 3d 355, 360–61 (1985). In Ribas, for instance, the defendant was a friend of the plaintiff's wife who eavesdropped on a phone conversation between the plaintiff and his wife and later testified to what she heard during an arbitration hearing. Id. at 358. The Court held that the complaint properly charged the defendant under section 631 because the legislature intended to prevent "eavesdropping, or the secret monitoring of conversations

by third parties." Id. at 359. But one cannot "eavesdrop" on their own conversation, and "it is never a secret to one party to a conversation that the other party is listening to the conversation." Rogers v. Ulrich, 52 Cal. App. 3d 894, 899 (1975). Thus, a participant to a conversation who uses a tape recorder to record the communication, even surreptitiously, is not liable under section 631. Id. at 897.

***3** To evaluate whether a software service provider like ActiveProspect constitutes a third-party listener as opposed to a participant in the conversation, courts assess whether the software service "extends beyond the ordinary function of a tape recorder." Yoon v. Lululemon USA, Inc. 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021); see also Javier v. Assurance IQ, LLC, 649 F. Supp. 3d 891, 898 (N.D. Cal. 2023) ("the Court must decide whether ActiveProspect is more akin to the tape recorder in Rogers, held by Assurance, or the friend in Ribas (in which case, Assurance is the wife who allowed ActiveProspect to listen in)"). This requires looking at the software vendor's independent "capability to use its record of the interaction for [another] purpose." Cody v. Ring LLC, 718 F. Supp. 3d 993, 1002 (N.D. Cal. 2024) (quoting Javier, 649 F. Supp. 3d at 900).

For example, if software essentially functions as a wiretap that redirects a plaintiff's communications with a website page to a marketing company that can use the data for its own ends, under section 631, the marketing company is not a party to the communication. See Revitch v. New Moosejaw, LLC, No. 18-CV-06827-VC, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 23, 2019) (denying motion to dismiss where plaintiff alleged that the embedded software code redirected website interactions to a third-party in real time); In re Facebook, Inc., 956 F.3d at 607–08 (denying motion to dismiss where Facebook used software to track interactions between Facebook users' browsers and other websites).

Conversely, if software functions only as a tool that, like a tape recorder, allows participants to record and analyze the contents of their own communications, the software vendor is not a third-party and no liability attaches. In Graham v. Noom, for example, the court held that software used to capture data on behalf of a website owner functioned as a mere recording tool because plaintiff did not allege that the software vendor "intercepted and used the data itself." 533 F. Supp. 3d 823, 832–33 (N.D. Cal. 2021). Critically, though, to establish liability under section 631 a plaintiff need only show that the software vendor is capable of using the data it collects for some other purpose; there is no statutory requirement that the vendor actually did so. See Javier, 649 F. Supp. 3d at 900. Therefore, a software vendor may be considered a third party even if it merely provides recording and transmission services to a party to the communication. See Saleh v. Nike, Inc., 562 F. Supp. 3d 503, 521 (C.D. Cal. 2021).

Defendants argue that ActiveProspect is not a third-party eavesdropper because ActiveProspect cannot use TrustedForm Certificates for any independent purpose. Mot. at 13–19. Defendants provide two reasons why: First, ActiveProspect does not have the ability to locate particular TrustedForm Certificates or link them with specific website users without the associated TrustedForm Certificate URL, which is held by the website owner, not ActiveProspect. See Ex. 22 (Retrieving a Retained TrustedForm Certificate) (dkt. 93-23) at 1 ("TrustedForm does not support searching for certificates based on lead data and thus cannot retroactively match lead data to a unique certificate."). Although ActiveProspect keeps a list of TrustedForm Certificate URLs, it does not have an index with which to identify what website or certificate each URL corresponds to. Wolfe Decl. ¶ 39. Second, even with the associated TrustedForm Certificate URLs, ActiveProspect cannot retrieve large numbers of stored TrustedForm Certificates at one time. Id. ¶ 40–41. Defendants contend that these limitations make it impossible for ActiveProspect to use TrustedForm Certificates "for any purpose beyond providing the TrustedForm software service to accountholders." Mot. at 14.

***4** But ActiveProspect can access, and potentially use, the data collected by the TrustedForm software. Deposition testimony reveals that certain ActiveProspect employees with "superuser access" can independently view TrustedForm Certificates for customer support purposes. See Wolfe Dep. at 162:14–163:2; Williams Dep. at 168:8–19, 123:16–126:15, 128:1–12. These select ActiveProspect employees can log into the accounts of accountholders, such as Assurance, and view TrustedForm certificates and the session replays that contain user-submitted data. Williams Dep. at 125:16–128:7. The ActiveProspect website itself confirms this capability. See Ex. 8 (ActiveProspect Security) (dkt. 105-9) at 3 ("Our employees may occasionally need access to accounts for support or troubleshooting purposes."). [1]

This matters because the user-submitted information from the webform that is accessible through the session replays in TrustedForm Certificates qualifies as contents of a communication. See SAC ¶ 45. And the fact that superuser employees can access this sensitive information suggests that

it could be used for a purpose other than collection and storage—even if Plaintiffs have not shown that it has, in fact, been used for such a purpose. Wolfe Dep. at 162:21–163:2 ("ActiveProspect staff are able to, on a support basis, access the Assurance ... account, and in doing so, can pull up one of the certificates that they have stored in their account for the purpose of troubleshooting.").

Defendants respond that superuser employee access does not necessarily mean that ActiveProspect can use TrustedForm data for its own ends because "only a strictly limited subset of ActiveProspect employees" are granted superuser access and those employees may access a TrustedForm Certificate "only at the request of the Certificate's owner" and "only for 'support or troubleshooting purposes.' " Reply (dkt. 124) at 7 (citation omitted) (emphasis in original). Defendants emphasize that ActiveProspect cannot use the TrustedForm data for its own purposes because such use is explicitly barred by the End User License Agreement (EULA) between ActiveProspect and Assurance. Id.; Mot. at 18 (citing EULA (dkt. 93-10) at 2, 4). [2]

Defendant's arguments are unpersuasive because they demonstrate only that it is ActiveProspect's policy not to use the TrustedForm data for its own purposes. This is irrelevant to the issue as to whether ActiveProspect is capable of using superuser access for its own ends. The fact remains that, if ActiveProspect can grant a limited subset of employees access to TrustedForm accounts (and, thus, the underlying TrustedForm data), then ActiveProspect can potentially use TrustedForm data for its own ends, even if it is not their policy to do so. [3]

***5** In short, ActiveProspect did not become a party to the webform communications simply because it was providing recording services to Assurance. See Saleh, 562 F. Supp. 3d at 521. Evidence in the record indicates that at least some ActiveProspect employees can view TrustedForm Certificates and session replays, so there is a genuine dispute of material fact as to whether ActiveProspect functions as more than a mere tape recorder. Accordingly, summary judgment is not appropriate on this basis.

B. Whether Defendants "Read" or "Attempted to Read" Communications

Defendants further argue that there is no genuine dispute about whether ActiveProspect read, attempted to read, or to learn the contents of Plaintiff's communications while they were in transit. This is a requirement under section 631. Though section 631 does not define "read" or "attempt to read," courts generally conclude that liability under prong two of section 631 "requires some effort at understanding the substantive meaning of the message, report or communication." E.g., Williams v. DDR Media, LLC, No. 22-CV-03789-SI, 2024 WL 4859078, at *5 (N.D. Cal. Nov. 20, 2024). A party to a communication "recording a conversation with a device and later sharing the recording with others is not a [section 631] violation." Valenzuela v. Nationwide Mut. Ins. Co., 686 F. Supp. 3d 969, 980 (C.D. Cal 2023) (citing Rogers, 52 Cal. App. 3d at 899). Defendants' argument prevails.

Plaintiffs argue that using "event listener" software to collect an interaction in real-time for the purpose of later reassembling a session replay constitutes an attempt to understand the content of that communication. Opp. at 22. According to Plaintiffs, section 631 liability attaches even if the "attempt" to understand the contents of a communication occurs when the contents are stored and no longer in transit. Id. Plaintiffs reiterate that Defendants could read encrypted certificate data before and after it was stored on the ActiveProspect server. Id. at 24. Plaintiffs also point to the fact that ActiveProspect employees use the substantive contents of session replays to testify on behalf of clients like Prudential, arguing that this is analogous to the friend in Ribas who violated section 631 by listening to and then later testifying about a phone conversation between a husband and wife. See Opp. at 12.

Ultimately, Plaintiffs' arguments do not show a genuine dispute of a material fact. Even if TrustedForm software intercepts the contents of Plaintiffs' communications in real time and stores the recording on an ActiveProspect server that ActiveProspect employees can access, nothing in the record plausibly indicates that ActiveProspect reads or attempts to read the contents of the communication while they are in transit. See Valenzuela v. Keurig Green Mountain, Inc., 674 F. Supp. 3d 751, 758 (N.D. Cal. 2023) (" 'While' is the key word here."). Webform inputs are collected and stored as a series of undeciphered "events," which are then provided to host websites to interpret using the ActiveProspect server. Wolfe Decl. ¶ 18. As explained above, ActiveProspect employees with "superuser access" can later access these communications and even testify to their contents, but there is no evidence in the record that those employees (or others) access communications while they are in transit. Whether Defendants access or even analyze inputs with Prudential's

consent after they have been transmitted to the server and reassembled has no bearing on whether Defendants read the communications while they were in transit. [4]

***6** Plaintiffs correctly point out that the legislature intended CIPA to be interpreted broadly to account for new technologies. Opp. at 9. But even applying the statute broadly, the record is devoid of evidence that ActiveProspect used technology to independently interpret the substantive meaning of communications while they were in transit. See R.C. v. Sussex Publishers, LLC, No. 24-CV-02609-JSC, 2025 WL 948060, at *7 (N.D. Cal. Mar. 28, 2025) (dismissing section 631 claim where technology is used to view, read, and process data only after it is stored). Plaintiffs suggest that a strict interpretation of the while-in-transit requirement would mean that CIPA could never apply in the context of the internet, where communications are near instantaneous and cannot be meaningfully read or understood until later. Whether or not that is true, it would stretch CIPA's statutory language too far to interpret "while ... in transit" to encompass any hypothetical future attempt to read or understand the meaning of a communication. [5]

Plaintiffs also argue that reassembling events into a session replay constitutes an attempt to understand the meaning of webform inputs. Opp. at 22. In re Facebook is again instructive. In that case, Facebook used plug-ins to track users' browsing histories, which it then used to create personal profiles that could be sold to advertisers. 956 F.3d at 596. The court affirmed that this adequately alleged conduct that amounted to a violation under CIPA. Id. at 607–08. Here, by contrast, ActiveProspect does not appear to analyze, summarize, or otherwise interpret Plaintiffs' data: the session replays on the ActiveProspect server are nothing more than a rote list of the actions that TrustedForm users took while filling out the form. The act of reassembling events like keystrokes, mouse movements, and clicks into a session replay (for the convenience of a party to the communication itself) is not analogous to creating personal profiles that can then be marketed to third-party advertisers. And it does not constitute reading under the statute, because reading requires an attempt to understand or interpret the substantive meaning of a communication, and the events recorded by TrustedForm do not become readable content until after they are stored and reassembled into a TrustedForm session replay. Even when a session replay is reassembled, it is done mechanically and without any attempt to decode its underlying meaning. Wolfe Decl. ¶¶ 18, 28.

To be sure, Plaintiffs demonstrate that ActiveProspect could have learned the substantive meaning of TrustedForm Certificates by accessing client accounts or viewing event log files. See Wolfe Dep. at 162:14–163:2; Shafiq Rpt. ¶¶ 88, 92–93. [6] But what ActiveProspect could do is not the relevant inquiry here—as opposed to the earlier analysis as to whether ActiveProspect functioned more like a tape recorder or a third-party eavesdropper. See James v. Allstate Ins. Co., No. 23-CV-01931-JSC, 2023 WL 8879246, at *3 (N.D. Cal. Dec. 22, 2023) ("Plaintiff's allegation that ... 'data is stored or can be accessed by [Defendant]' is insufficient to support a plausible inference [Defendant] attempted to read or learn the contents of the communication while in transit."). The question is whether ActiveProspect did independently attempt to decipher the contents of any communication. And Plaintiffs fail to provide any evidence indicating that ActiveProspect did so.

***7** Separately, Plaintiffs argue that the TrustedForm software functionally reads the data when it detects email addresses and phone numbers that require "normaliz[ing] and hash[ing]" to be operative for certain features of the TrustedForm software. Opp. at 23 (citing Williams Dep. at 174:15–20). Plaintiffs assert that "categorizing and analyzing" information using TrustedForm software prior to transmission also constitutes an attempt to understand its meaning. Opp. at 23. No reasonable jury could agree. Whether an input is normalized and hashed depends on a set of pre-determined criteria that is mechanically deployed with no intelligible understanding of those values required. See Williams, 2024 WL 4859078, at *5 (holding that the hashing process, during which original data is formatted in a particular way, does not constitute "reading" under CIPA).

Because Plaintiffs have not shown that ActiveProspect attempted to understand or decipher the contents of Plaintiffs' communications on its webform while the communications were in transit, there is no genuine dispute as to whether ActiveProspect read or attempted to read those communications under section 631. Further, because there is no predicate violation of section 631 on the part of ActiveProspect, there is no genuine dispute as to whether Prudential and Assurance aided and abetted ActiveProspect in violation of section 631.

IV. CONCLUSION

For the foregoing reasons, this Court **GRANTS** Defendants' motion for summary judgment.

IT IS SO ORDERED.

All Citations

Slip Copy, 2025 WL 1135088

Footnotes

1 Plaintiffs cite a report by Professor Zubair Shafiq, an internet privacy and security expert, opining that files containing event logs are stored on the server in decoded plain text form, which would allow ActiveProspect to access the content of encoded and encrypted TrustedForm Certificates. Shafiq Rpt. (dkt. 105-7) ¶¶ 88, 92–93. Defendants challenge Shafiq's expert report. Mot. to Exclude (dkt. 122). Because other evidence in the record creates a genuine dispute as to whether ActiveProspect is capable of using TrustedForm data for its own ends, Defendants' motion to exclude Shafiq's report is moot.

2 Defendants argue that the EULA between ActiveProspect and Assurance regarding the use of TrustedForm confirms ActiveProspect's inability to use TrustedForm data for its own ends because ActiveProspect's "right to use aggregate data" under the EULA refers only to metadata, not user-submitted data. Mot. at 18 (citing EULA at 2, 4). But ActiveProspect's Terms of Service for all ActiveProspect products explicitly reserves its right to use collected content and data that "potentially includes personally identifiable information." Rafferty Dep. at 151:11–20; see also Terms of Service (dkt. 105-10) at 9. Therefore, at the summary judgment stage, Defendants have not proven that no genuine dispute exists as to whether they can use the TrustedForm data for their own ends.

3 In their Reply, Defendants cite several cases where district courts concluded that data collected using certain software could not reasonably be used by the software vendor for another purpose. See Reply at 7. Those cases are readily distinguishable. See Yockey v. Salesforce, Inc., 688 F. Supp. 3d 962, 973 (N.D. Cal. 2023) (data at issue were transcripts of customer support communications, not medical histories and contact information); Heiting v. athenahealth, Inc., No. 2:23-CV-10338-FLA (DFMX), 2024 WL 3761294, at *4 (C.D. Cal. July 29, 2024) (allegations as to access were "general and conclusory"); Gutierrez v. Converse Inc., No. CV 23-6547-KK-MARX, 2024 WL 3511648, at *6 (C.D. Cal. July 12, 2024) (access could only be provided by the accountholder).

4 During oral argument Plaintiffs cited People v. Otto, 2 Cal. 4th 1088 (1992), to posit that CIPA applies even where a conversation is recorded at one time and listened to (in an attempt to read or understand it) at a later time. But Otto involved the federal wiretapping statute, 18 U.S.C. § 2511, not CIPA. Id. at 1098. And in any case, the parties in Otto did not argue, and the court therefore did not address, whether anyone read or attempted to read the relevant communications while they were in transit.

5 Consider two examples. In In re Facebook, Facebook was alleged to have used browser plug-ins to "replicate and send [ ] user data to Facebook through a separate, but simultaneous, channel," at which point Facebook "compiled the [data] it collected into personal user profiles." 956 F.3d at 596. And in In re Google Inc., Google was alleged to have "intercepted, read and acquired the content of emails that were sent or received by Gmail user[s] while the emails were in transit ... for the purposes of sending an advertisement relevant to that email communication." No. 13-md-2430-LHK, 2013 WL 5423918, at *1 (N.D. Cal. Sept. 26, 2013). Both courts denied motions to dismiss the section 631 claims. In re Facebook, 956 F.3d at 606–08; In re Google, 2013 WL 5423918, at *19–22. As these cases illustrate, CIPA remains perfectly viable in the context of internet communications.

6 Though ActiveProspect concedes that there were instances when certain employees accessed customers' accounts and viewed TrustedForm certificates and session replays, the employees only did so in response to customer requests for support and troubleshooting. See Williams Dep. at 123:16–128:12. This does not give rise to section 631 liability because a party to a communication—in this case the TrustedForm accountholder—is permitted to record the communication and later show it to a third-party. See Valenzuela, 686 F. Supp. 3d at 980.

End of Document